JOURNAL OF NUMBER THEORY **65**, 87–95 (1997)
ARTICLE NO. NT972133

Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger

Bouchaïb Sodaïgui

Département de Mathématiques, Université de Valenciennes, Le Mont Houy, B.P. 311, 59304 Valenciennes Cedex, France

Communicated by W. Sinnott

Received March 16, 1996

Let k be a number field, O_k its ring of integers, Γ a nonabelian metacyclic group
[illegible]
containing $O_k[\Gamma]$, $\mathscr{C}\ell(\mathscr{M})$ its class group. We determine the set of elements of $\mathscr{C}\ell(\mathscr{M})$ which are realizable by some tamely ramified extensions with Galois groups isomorphic to Γ using some Stickelberger elements, and we prove that it is a subgroup of $\mathscr{C}\ell(\mathscr{M})$. © 1997 Academic Press

INTRODUCTION

Soient k un corps de nombres et O_k son anneau des entiers. Soient Γ un groupe fini, N/k une extension galoisienne à groupe de Galois isomorphe à Γ, et O_N son anneau des entiers. Soit $\mathscr{M}$ un ordre maximal de O_k dans l'algèbre semi-simple $k[\Gamma]$ contenant $O_k[\Gamma]$. Lorsque N/k est modérement ramifiée on peut associer à O_N une classe, notée $[O_N]$, dans $\mathscr{C}\ell(O_k[\Gamma])$, le groupe des classes de $O_k[\Gamma]$, et par extension des scalaires une classe, notée aussi $[O_N]$, dans $\mathscr{C}\ell(\mathscr{M})$ le groupe des classes de $\mathscr{M}$.

On désigne par $\mathscr{R}(O_k[\Gamma])$ (resp. $\mathscr{R}(\mathscr{M})$) l'ensemble des classes c de $\mathscr{C}\ell(O_k[\Gamma])$ (resp. $\mathscr{C}L(\mathscr{M})$) telle qu'il existe une extension N/k modérement ramifiée, à groupe de Galois isomorphe à Γ, avec $[O_N]=c$; on dira que c est réalisable par l'extension N/k et $\mathscr{R}(O_k[\Gamma])$ (resp. $\mathscr{R}(\mathscr{M})$) est l'ensemble des classes réalisables.

Lorsque Γ est abélien et k un corps de nombres quelconque, McCulloh [Mc] a décrit $\mathscr{R}(O_k[\Gamma])$ en utilisant une "correspondance de Stickelberger," ce qui lui a permis de montrer que $\mathscr{R}(O_k[\Gamma])$ est un sous-groupe de $\mathscr{C}\ell(O_k[\Gamma])$.

Dans cet article, on s'intéresse au cas non abélien. On se place dans la situation suivante: Γ est un groupe métacyclique d'ordre lq, où l et q sont

0022-314X/97 $25.00

deux nombres premiers, et k est linéairement disjoint de $\mathbb{Q}(\xi_l, \xi_q)$, où ξ_l (resp. ξ_q) est une racine primitive $l^{\text{ième}}$ (resp. $q^{\text{ième}}$) de l'unité. Le résultat principal est la description de $\mathcal{R}(\mathcal{M})$ à l'aide de deux idéaux de Stickelberger et on montre que $\mathcal{R}(\mathcal{M})$ est un sous-groupe de $\mathcal{C}L(\mathcal{M})$.

I. ÉNONCÉ DU RÉSULTAT PRINCIPAL

Un groupe métacyclique Γ non abélien d'ordre lq possède la structure suivante: il est engendré par deux éléments σ et τ, σ est un générateur d'un sous-groupe distingué de Γ, noté C_l, d'ordre l, et τ d'un sous-groupe de Γ d'ordre q, noté C_q; on a en plus la relation: $\tau\sigma\tau^{-1} = \sigma^r$, où r est un entier vérifiant les conditions suivantes: $1 < r \leqslant l-1$ et $r^q \equiv 1(l)$, un tel groupe n'est donc défini que si $l \equiv 1(q)$, et il est le produit semi direct de C_q par C_l. On désigne par K le sous-corps de $k(\xi_l)$ tel que le degré de l'extension $k(\xi_l)/K$ est égal à q. La décomposition de l'algère semi-simple $k[\Gamma]$ en un produit d'algères simples est la suivante: [cf. [Y]] $k[\Gamma] \simeq k \times k(\xi_q) \times M_q(K)$; où $M_q(K)$ est l'anneau des matrices d'ordre q à coefficients dans K.

Soit $\mathcal{M}$ un ordre maximal de O_k dans $k[\Gamma]$ contenant $O_k[\Gamma]$. Il est clair que le completé d'une composante simple de $k[\Gamma]$ à une éventuelle place réelle ne peut-être isomorphe à une algèbre de matrices sur le corps de quaternions sur $\mathbb{R}$. On a donc:

$$\mathcal{C}\ell(\mathcal{M}) \simeq \mathcal{C}\ell(k) \times \mathcal{C}\ell(k(\xi_q)) \times \mathcal{C}\ell(K);$$

où $\mathcal{C}\ell(k)$, $\mathcal{C}\ell(k(\xi_q))$ et $\mathcal{C}\ell(K)$ désignent les groupes des classes respectifs des idéaux fractionnaires de k, $k(\xi_q)$ et K.

L'extension $k(\xi_l)/k$ (resp. $k(\xi_q)/k$) est galoisienne et son groupe de Galois, noté S_l (resp. S_q), est isomorphe par restriction à celui de $\mathbb{Q}(\xi_l)/\mathbb{Q}$ (resp. $\mathbb{Q}(\xi_q)/\mathbb{Q}$); les éléments de S_l (resp. S_q) sont les éléments s_i (resp. s'_i), $1 \leqslant i \leqslant l-1$ (resp. $1 \leqslant i \leqslant q-1$), définis par: $s_i(\xi_l) = \xi_l^i$ (resp. $s'_i(\xi_q) = \xi_q^i$). Soit θ_l (resp. θ_q) l'élément de Stickelberger défini par $\theta_l = \sum_{i=1}^{l-1} is_i^{-1}$ (resp. $\theta_q = \sum_{i=1}^{q-1} is_i'^{-1}$). On appelle idéal de Stickelberger associé à l (resp. q) l'idéal $\mathcal{S}_l$ (resp. $\mathcal{S}_q$) de $\mathbb{Z}[S_l]$ (resp. $\mathbb{Z}[S_q]$) défini par:

$$\mathcal{S}_l = \frac{1}{l}\,\theta_l \mathbb{Z}[S_l] \cap \mathbb{Z}[S_l]$$

et

$$\mathcal{S}_q = \frac{1}{q}\,\theta_q \mathbb{Z}[S_q] \cap \mathbb{Z}[S_q].$$

On appellera élément de Stickelberger tout élément de $\mathcal{S}_l$ ou $\mathcal{S}_q$.

On munit le groupe $I_{k(\xi_q)}$ des idéaux fractionnaires de $k(\xi_q)$ de la structure de $\mathbb{Z}[S_q]$ module définie par: pour tout $I \in I_{k(\xi_q)}$, on pose

$$\left(\sum_{i=1}^{q-1} a_i s'_i\right) I = \prod_{i=1}^{q-1} s'_i(I)^{a_i},$$

ce qui donne une structure de $\mathbb{Z}[S_q]$-module sur $\mathscr{C}\ell(k(\xi_q))$.

L'extension K/k étant galoisienne, le groupe S_l opère, par restriction, sur I_K le groupe des idéaux fractionnaires de K d'une manière analogue à ci-dessus, ce qui donne aussi une structure de $\mathbb{Z}[S_l]$ module sur $\mathscr{C}\ell(K)$.

Le principal résultat est le théorème suivant:

Théorème. *Notons $\mathscr{S}_q\mathscr{C}\ell(k(\xi_q))$ (resp. $\mathscr{S}_l\mathscr{C}\ell(K)$) le sous groupe de $\mathscr{C}\ell(k(\xi_q))$ (resp. $\mathscr{C}\ell(K)$) engendré par les éléments de la form $\mathscr{A}X$, $\mathscr{A} \in \mathscr{S}_q$ (resp. $\mathscr{S}_l$) et $X \in \mathscr{C}\ell(k(\xi_q))$ (resp. $\mathscr{C}\ell(K)$). Alors, $\mathscr{R}(\mathscr{M})$ est un groupe isomorphe au groupe produit: $\mathscr{S}_q\mathscr{C}\ell(k(\xi_q)) \times \mathscr{S}_l\mathscr{C}\ell(K)$.*

II. DESCRIPTION D'UN REPRÉSENTANT DE O_N DANS $\mathscr{C}\ell(\mathscr{M})$.

Soit R_Γ le groupe abélien libre engendré par les caractères absolument irréductibles de Γ. Le groupe Γ étant le produit semi-direct d'un sous-groupe C_q d'ordre q par un sous-groupe C_l distingué d'ordre l, il possède donc (cf. [S, Chap. II, Sect. 8]) trois classes de conjugaisons de caractères absolument irréductibles dont les représentants sont les suivants:

(a) χ_0 est le caractère trivial de Γ.

(b) χ_1 est un caractère non trivial, de degré 1, dont le noyau est C_l.

(c) χ_2 est un caractère de degré q, qui est induit par un caractère non trivial φ de C_l, de degré 1, i.e. $\chi_2 = \mathrm{Ind}_{C_l}^{\Gamma} \varphi$.

Soient $\bar{k}$ une clôture algébrique de k, $\Omega_k = \mathrm{Gal}(\bar{k}/k)$, $J(\bar{k})$ le groupe des idèles de $\bar{k}$. On désigne par $U(\bar{k})$ les idèles de $J(\bar{k})$ qui sont des unités aux places finies et $\bar{k}^* = \bar{k} - \{0\}$. D'après les travaux de Fröhlich ([F, 1]) on a:

$$\mathscr{C}\ell(\mathscr{M}) \simeq \frac{\mathrm{Hom}_{\Omega_k}(R_\Gamma, J(\bar{k}))}{\mathrm{Hom}_{\Omega_k}(R_\Gamma, \bar{k}^*) \times \mathrm{Hom}_{\Omega_k}(R_\Gamma, U(\bar{k}))}.$$

Définition des résolvantes de Lagrange (cf. [F, 1]):

Soit E/F une extension galoisienne de degré fini, de groupe de Galois isomorphe à Γ, B une F-algèbre commutative; $E \otimes_F B$ est un $B[\Gamma]$-module libre de rang 1.

DÉFINITION 2.1. Soit a une base du $B[\Gamma]$-module $E \otimes_F B$, T une représentation de $\Gamma \to GL_n(\bar{k})$ de caractère χ. On appelle résolvante de Lagrange de a et de χ l'élément $<a, \chi>$ défini par:

$$\langle a, \chi \rangle = \mathrm{Det}\left(\sum_{\gamma \in \Gamma} \gamma(a)\, T(\gamma^{-1}) \right)$$

où Det désigne le déterminant.

Remarques. (a) Soit π un isomorphisme de $\mathrm{Gal}(E/F)$ dans Γ, $\gamma(a)$ veut dire $\pi^{-1}(\gamma)(a)$.

(b) Lorsque l'on veut préciser d'avantage, on écrit $\langle a, \chi \rangle_{E/F}$ au lieu de $\langle a, \chi \rangle$.

Notations. Dans la suite p désigne un ideál premier quelconque de O_k, k_p (resp. $O_{k,p}$) la complétion de k (resp. O_k) en p. Si L est un corps de nombres contenant k et O_L son anneau des entiers, on notera: $L_p = L \otimes_k k_p$ et $O_{L,p} = O_L \otimes_{O_k} O_{k,p}$.

THÉORÈME 2.2 (cf. [F, 1]). *Soit N/k une extension galoisienne modérément ramifiée et à groupe de Galois isomorphe à Γ. Soit a une base du $k[\Gamma]$-module N. Pour tout idéal premier p de O_k, soit α_p une base du $O_{k,p}[\Gamma]$-module $O_{N,p}$. Alors, un représentant de $[O_N]$ dans $\mathscr{C}\ell(\mathscr{M})$ est l'application f définie par*:

$$f(\chi) = \left(\frac{\langle \alpha_p, \chi \rangle}{\langle a, \chi \rangle} \right).$$

Dans ce qui suit, on va déterminer un élément g de $\mathrm{Hom}_{\Omega_k}(R_\Gamma, J(\bar{k}))$ qui représente O_N dans $\mathscr{C}\ell(\mathscr{M})$, en donnant les valeurs qu'il prend en χ_0, χ_1, et χ_2. Les notations a et α_p sont celles du théorème.

Il est clair que $\langle \alpha_p, \chi_0 \rangle = \mathrm{Tr}_{N_p/k_p}(\alpha_p)$ et que $\langle a, \chi_0 \rangle = \mathrm{Tr}_{N/k}(a)$ (où Tr désigne la trace). On peut supposer que $\mathrm{Tr}_{N/k}(a) = 1$ (prendre $a/\mathrm{Tr}_{N/k}(a)$ sinon). Comme α_p est une base normale d'entiers, $\mathrm{Tr}_{N_p/k_p}(\alpha_p)$ est une unité de $O_{k,p}$, et on peut choisir α_p de telle sorte que $\mathrm{Tr}_{N_p/k_p}(\alpha_p) = 1$. On pose alors $g(\chi_0)_p = 1$.

La restriction de χ_1 à C_q définit un caractère de degré 1 de C_q non trivial qu'on note $\underline{\chi_1}$. Les égalités suivantes découlent facilement de la définition des résolvantes de Lagrange, où k' est le sous corps de N invariant par C_l:

$$\langle \alpha_p, \chi_1 \rangle = \langle \mathrm{Tr}_{N_p/k'_p}(\alpha_p), \underline{\chi_1} \rangle_{k'/k} \tag{2.1}$$

$$\langle a, \chi_1 \rangle = \langle \mathrm{Tr}_{N/k'}(a), \underline{\chi_1} \rangle_{k'/k}. \tag{2.2}$$

Signalons que $\mathrm{Tr}_{N_p/k'_p}(\alpha_p)$ et $\mathrm{Tr}_{N/k'}(a)$ sont des bases respectives du $O_{k,p}[C_q]$-module $O_{k',p}$ et du $k[C_q]$-module k'.

On pose

$$g(\chi_1)_p = \frac{\langle \mathrm{Tr}_{N_p/k'_p}(\alpha_p), \underline{\chi_1} \rangle_{k'/k}}{\langle \mathrm{Tr}_{N/k'}(a), \underline{\chi_1} \rangle_{k'/k}}. \tag{2.3}$$

Un théorème de Fröhlich (cf. [F, 2, Théorème 12]), donne le lien entre la résolvante d'un caractère d'un sous-groupe de Γ et la résolvante de l'induction de ce même caractère à Γ. Dans notre situation, où l'on a posé $\chi_2 = \mathrm{Ind}_{C_l}^{\Gamma} \varphi$ on a:

Soit b et b_p des bases respectives du $k'[C_l]$-module N et du $O_{k',p}[C_l]$-module $O_{N,p}$. Il existe λ et λ_p des éléments inversibles respectifs des anneaux $k[C_l]$ et $O_{k,p}[C_l]$ tels que:

$$\langle a, \chi_2 \rangle\ \varphi(\lambda) = N_{k'/k}[\langle b, \varphi \rangle_{N/k'}]\ e(k'/k) \tag{2.4}$$

et

$$\langle \alpha_p, \chi_2 \rangle\ \varphi(\lambda_p) = N_{k'/k}[\langle b_p, \varphi \rangle_{N/k'}]\ e(k'_p/k_p);$$

où l'on a prolongé φ par linéarité à $k_p[C_l]$, $e(k'/k)^2$ et $e(k'_p/k_p)^2$ sont les discriminants respectifs de k'/k et k'_p/k_p, et

$$N_{k'/k}\langle x, \varphi \rangle = \prod_{\gamma \in \mathrm{Gal}(k'/k)} \gamma \langle x, \gamma^{-1}\varphi \rangle;$$

dans notre situation $N_{k'/k}\langle x, \varphi \rangle = \prod_{\gamma \in \mathrm{Gal}(k'/k)} \gamma\langle x, \varphi \rangle$ car $\mathrm{Gal}(k'/k)$ laisse invariant ξ_l. Les égalités (2.4) entrainent:

$$\frac{\langle \alpha_p, \chi_2 \rangle}{\langle a, \chi_2 \rangle} = \varphi(\lambda)^{-1}\ \varphi(\lambda_p) \cdot \frac{e(k'_p/k_p)}{e(k'/k)}\ N_{k'/k}\left[\frac{\langle b_p, \varphi \rangle_{N/k'}}{\langle b, \varphi \rangle_{N/k'}}\right].$$

On pose

$$g(\chi_2)_p = N_{k'/k}\left[\frac{\langle b_p, \varphi \rangle_{N/k'}}{\langle b, \varphi \rangle_{N/k'}}\right]. \tag{2.5}$$

D'une part, l'application définie sur R_Γ et à valeurs dans $\bar{k}^*$ qui à χ_0 et χ_1 associe 1, et qui à χ_2 associe $\varphi(\lambda)$, est un élément de $\mathrm{Hom}_{\Omega_k}(R_\Gamma, \bar{k}^*)$.

D'autre part, comme $e(k'/k) = \prod_p e(k'_p/k_p)$, l'élément $e(k'_p/k_p)/e(k'/k)$ est une unité locale en p, et l'application définie sur R_Γ et à valeurs dans $U(\bar{k})$ qui à χ_0 et χ_1 associe 1 et à χ_2 associe $\varphi(\lambda_p) = e(k'_p/k_p)/e(k'/k)$ appartient à $\mathrm{Hom}_{\Omega_k}(R_\Gamma, U(\bar{k}))$. En résumé, on a donc la proposition suivante:

PROPOSITION 2.3. *Sous les hypothèses et les notations définies ci-dessus, on a: Soit g l'élément de* $\mathrm{Hom}_{\Omega_k}(R_\Gamma, J(\bar{k}))$ *défini par: pour tout idéal premier p de O_k,*

$$g(\chi_0)_p = 1, \qquad g(\chi_1)_p = \frac{\langle \mathrm{Tr}_{N_p/k'_p}(\alpha_p), \underline{\chi_1} \rangle_{k'/k}}{\langle \mathrm{Tr}_{N/k'}(a), \underline{\chi_1} \rangle_{k'/k}}$$

$$g(\chi_2)_p = N_{k'/k} \frac{\langle b_p, \varphi \rangle_{N/k'}}{\langle b, \varphi \rangle_{N/k'}}.$$

Alors, la classe de O_N dans $\mathcal{C}\ell(\mathcal{M})$ est égale à la classe de g dans $\mathcal{C}\ell(\mathcal{M})$.

On va maintenant déterminer effectivement des idéaux fractionnaires respectifs de O_k, $O_{k(\xi_q)}$, et O_K qui représentent O_N dans $\mathcal{C}\ell(k) \times \mathcal{C}\ell(k(\xi_q)) \times \mathcal{C}\ell(K)$, grâce à la proposition ci-dessus, et à [SO].

Soit $\bar{\tau}$ un prolongement de τ à $k'(\xi_l)$, on note k'_r le sous corps de $k'(\xi_l)$ fixe par $\bar{\tau} s_r$. Soit M un sous corps de N de degré l sur k, d'après [P] on peut choisir $b \in M$. On a la décomposition d'une manière unique suivante (cf. [SO, théorème 5.2]; les résultats de la section 5 sont encore vrais si l'on remplace $\mathbb{Q}$ par un corps linéairement, disjoint de $\mathbb{Q}(\xi_l)$ sur $\mathbb{Q}$):

$$\langle \mathrm{Tr}_{N/k'}(a), \underline{\chi_1} \rangle_{k'/k}^{q} O_{k(\xi_q)} = I(\underline{\chi_1})^q \, \theta_q \, J(\underline{\chi_1}),$$

$$\langle b, \varphi \rangle_{N/k'}^{l} O_{k'_r} = I(\varphi)^l \, \theta_l \, J(\varphi),$$

où $I(\underline{\chi_1})$ (resp. $I(\varphi)$) est un idéal fractionnaire de $k(\xi_q)$ (resp. k'_r), et $J(\underline{\chi_1})$ (resp. $J(\varphi)$) est un idéal entier de $k(\xi_q)$ (resp. k'_r), sans facteur carré et tel que les idéaux $s'_i(J(\underline{\chi_1}))$ (resp. $s_i(J(\varphi))$, $1 \leqslant i \leqslant q-1$ (resp. $1 \leqslant i \leqslant l-1$), soient premiers entre eux deux à deux.

PROPOSITION 2.4. *La classe de O_N dans $\mathcal{C}\ell(\mathcal{M})$ est représentée par:*

(i) *La classe triviale dans $\mathcal{C}\ell(k)$.*

(ii) *La classe de $I(\underline{\chi_1})^{-1}$ dans $\mathcal{C}\ell(k(\xi_q))$.*

(iii) *La classe de $N_{k'_r/K}(I(\varphi)^{-1})$ dans $\mathcal{C}\ell(K)$; où $N_{k'_r/K}$ désigne la norme dans k'_r/K.*

Démonstration. Il est évident que la classe de O_N est représentée par la classe triviale dans $\mathcal{C}\ell(k)$, d'après la proposition 2.3, d'où (i).

Les extensions N/k' et k'/k sont modérément ramifiées car N/k est modérément ramifiée.

Soit $\mathcal{M}_1$ (resp. $\mathcal{M}_2$) l'ordre maximal de O_k (resp. $O_{k'}$) dans $k[C_q]$ (resp. $k'[C_l]$) contenant $O_k[C_q]$ (resp. $O_{k'}[C_l]$). Il est clair que l'élément g_1 de $\mathrm{Hom}_{\Omega_k}(R_{C_q}, J(\bar{k}))$, où R_{C_q} est le groupe des caractères virtuels de C_q, qui au caractère trivial de C_q associe 1 et à $\underline{\chi_1}$ associe $g_1(\underline{\chi_1})=g(\chi_1)$, est un représentant de $O_{k'}$ dans le groupe des classes de $\mathcal{M}_1$, $\mathcal{C}\ell(\mathcal{M}_1)$, qui est isomorphe à $\mathcal{C}\ell(k)\times\mathcal{C}\ell(k(\xi_q))$; d'après le théorème 2.3 de [SO] la classe de $O_{k'}$ dans $\mathcal{C}\ell(k(\xi_q))$ est égale à la classe de $I(\underline{\chi_1})^{-1}$, mais la classe de $O_{k'}$ dans $\mathcal{C}\ell(k(\xi_q))$ est égale à la classe de O_N dans $\mathcal{C}\ell(k(\xi_q))$ d'après la proposition 2.3 d'où (ii).

Soit, maintenant, g_2 l'élément de $\mathrm{Hom}_{\Omega_{k'}}(R_{C_l}, J(\bar{k}))$, où $\Omega_{k'}=\mathrm{Gal}(\bar{k}/k')$ et R_{C_l} le groupe des caractères virtuels de C_l, qui au caractère trivial de C_l fait correspondre 1 et à φ fait correspondre $g_2(\varphi)$ défini par: pour tout idéal premier p de O_k, $g_2(\varphi)_p=\langle b_p, \varphi\rangle/\langle b, \varphi\rangle$; g_2 est un représentant de O_N dans le groupe des classes de $\mathcal{M}_2$. D'après [P], on peut choisir $b\in M$ et $b_p\in M_p$ où M est le sous corps de N fixe par τ. On vérifie facilement les propriétés suivantes:

$$\tau\langle b_p, \varphi\rangle=\langle\tau(b_p), \varphi^{r^*}\rangle \qquad \text{et} \qquad \tau\langle b, \varphi\rangle=\langle\tau(b), \varphi^{r^*}\rangle,$$

où r^* est l'inverse de r modulo l,

$$s_r\langle b_p, \varphi\rangle=\langle b_p, \varphi^r\rangle \qquad \text{et} \qquad s_r\langle b, \varphi\rangle=\langle b, \varphi^r\rangle,$$

$$\sigma\langle b_p, \varphi\rangle=\varphi(\sigma)\langle b_p, \varphi\rangle \qquad \text{et} \qquad \sigma\langle b, \varphi\rangle=\varphi(\sigma)\langle b, \varphi\rangle.$$

Mais τ laisse fixe M_p, on en déduit que $g_2(\varphi)_p\in k'_{r,p}$. Le théorème 5.2 de [SO] nous permet de dire qu'à $g_2(\varphi)$ correspond la classe de l'idéal $I(\varphi)^{-1}$ dans $\mathcal{C}\ell(k'_r)$. Comme $\mathrm{Gal}(k'_r/K)$ est isomorphe à $\mathrm{Gal}(k'/k)$ on a $N_{k'/k}(I(\varphi)^{-1})=N_{k'_r/K}(I(\varphi)^{-1})$ qui est donc un représentant de la classe de O_N, en tant que $O_k[\Gamma]$-module, dans $\mathcal{C}\ell(K)$, d'où (iii).

III. DÉMONSTRATION DU RÉSULTAT PRINCIPAL

La proposition 2.4, nous permet d'identifier $\mathcal{R}(\mathcal{M})$ avec un sous ensemble de $\mathcal{C}\ell(k(\xi_q))\times\mathcal{C}\ell(K)$. Pour la démonstration du résultat principal, on procèdera par double inclusion et on utilisera des résultats de [SO].

Proposition 3.1. *On a*:

$$\mathcal{R}(\mathcal{M})\subset\mathcal{S}_q\mathcal{C}\ell(k(\xi_q))\times\mathcal{S}_l\mathcal{C}\ell(K).$$

Démonstration. Les notations sont celles de la proposition 2.4. D'après [SO, Théorème 2.3 et Théorème 5.2], la classe de $I(\underline{\chi_1})^{-1}$ appartient à $\mathcal{S}_q\mathcal{C}\ell(k(\xi_q))$, et la classe de $I(\varphi)^{-1}$ appartient à $\mathcal{S}_l\mathcal{C}\ell(k'_r)$ et donc $N_{k'_r/K}(I(\varphi)^{-1})\in\mathcal{S}_l\mathcal{C}\ell(K)$; d'où la proposition.

PROPOSITION 3.2. *On a*:

$$\mathscr{R}(\mathscr{M}) \supset \mathscr{S}_q \mathscr{C}\ell(k(\xi_q)) \times \mathscr{S}_l \mathscr{C}\ell(K).$$

On a besoin du lemme suivant (cf. [W, Théorème 10.1]):

LEMME 3.3. *Soit L'/L une extension de corps de nombres telle qu'il existe une place de L totalement ramifiée dans L'. Alors, la norme dans L'/L induit un homomorphisme surjectif du groupe des classes des idéaux de L' dans le groupe des classes des idéaux de L.*

Démonstration de la proposition 3.2. Soit $(X, Y) \in \mathscr{S}_q \mathscr{C}\ell(k(\xi_q)) \times \mathscr{S}_l \mathscr{C}\ell(K)$. On considère tout d'abord X. D' après le théorème 2.4 de [SO], il existe une extension galoisienne k'/k, à groupe de Galois isomorphe à C_q modérément ramifiée, de degré q, telle que la classe de $O_{k'}$ l'anneau des entiers de k', dans $\mathscr{C}\ell(k(\xi_q))$ qui est l'une des deux composantes de l'ordre maximal de O_k dans $k[C_q]$ contenant $O_k[C_q]$, est égale à X. De plus [SO, Lemme 3.4], on peut supposer que k'/k est ramifiée au moins en une place finie.

On adjoint ξ_l à k'. On note τ un générateur de $\mathrm{Gal}(k'/k)$ et $\bar{\tau}$ un prolongement de τ à $k'(\xi_l)$. On note $\bar{s}_r$ un prolongement de $s_r \in \mathrm{Gal}(k(\xi_l)/k)$ à $k'(\xi_l)$, où r est un entier vérifiant $1 < r < l$ et $r^q \equiv 1(l)$. On désigne par k'_r le sous corps de $k'(\xi_l)$ invariant par $\bar{\tau}\bar{s}_r$. On considère maintenant Y. On va montrer que $N_{k'_r/K}$ induit un homomorphisme surjectif de $\mathscr{S}_l \mathscr{C}\ell(k'_r)$ sur $\mathscr{S}_l \mathscr{C}\ell(K)$, et donc il existe $Z \in \mathscr{S}_l \mathscr{C}\ell(k'_r)$ tel que $Y = N_{k'_r/K}(Z)$. En effet: On vérifie sans peine que $k'(\xi_l)/k'_r$ est non ramifiée en dehors des places finies différentes de l. Comme la seule place qui se ramifie dans K/k est l, k'/k est ramifiée au moins en une place, de plus k'_r/K est galoisienne de degré q, on a donc: k'_r/K est totalement ramifiée au moins en une place finie de K. On conclut grâce au lemme 3.3 et au fait que $\bar{\tau}$ commute avec les éléments de $\mathscr{S}_l((\mathrm{Gal}(k'_r/K) \simeq \langle \bar{\tau} \rangle)$.

On considère enfin Z. Soit I un ideal de k'_r qui représente Z. Le théorème 5.2 de [SO], nous affirme l'existence d'une extension N/k', galoisienne à groupe de Galois isomorphe à C_l, modérément ramifiée, telle que N/k est galoisienne à groupe de Galois isomorphe à Γ, et est modérément ramifiée car N/k' et k'/k le sont, et dont la classe de O_N l'anneau d'entiers de N, en tant que $O_{k'}[C_l]$-module, est égale à $\mathscr{C}\ell(IO_{k'(\xi_l)})$, où $O_{k'(\xi_l)}$ est l'anneau des entiers de $k'_{(\xi_l)}$. La proposition 2.4 nous dit que la classe de O_N, en tant que $O_k[\Gamma]$-module, dans $\mathscr{C}\ell(K)$ est égale à $N_{k'_r/K}\mathscr{C}\ell(I) = N_{k'_r/K}(Z) = Y$.

REMERCIEMENT

Ce travail a été réalisé totalement à l'université de Genève. Je saisis l'occasion de sa publication pour exprimer ma profonde reconnaissance à B. Erez, M. Kervaire, J. Queyrut, grâce à qui j'ai passé deux belles et inoubliables années de ma vie à Genève.

RÉFÉRENCES

[F, 1] A. Fröhlich, "Galois Module Structure of Algebraic Integers," Springer-Verlag, Berlin, 1983.

[F, 2] A. Fröhlich, Galois module structure, *in* "Algebraic Number Fields, Proceedings of the Durham Symposium, 1975," pp. 133–191, Academic Press, London, 1977.

[Mc] L. R. McCulloh, Galois module structure of abelian extensions, *J. Reine Angew. Math.* **375**/**376** (1987), 259–306.

[P] J.-J. Payan, Critère de décomposition d'une extension de Kummer sur un sous corps du corps de base, *Ann. Sci. École Norm. Sup.* **1** (1968), 445–458.

[S] J.-P. Serre, "Representation linéaire des groupes finis," Edition Hermann, Paris, 1971.

[SO] B. Sodaïgui, Structure galoisienne relative des anneaux d'entiers, *J. Number Theory* **28**, No. 2 (1988), 189–204.

[Y] T. Yamada, On the group algebras of metacyclic groups over algebraic number fields, *J. Fac. Sci. Univ. Tokyo* **15** (1969), 179–198.

[W] L. C. Washington, "Introduction to Cyclotonic Fields," Graduate Texts in Math., Vol. 83, Springer-Verlag, New York, 1982.